5. Del

Isogenies and rational points in char p

Version $-\infty$— last update: 10/5/14 1:48:46 PM
Preliminary version prone to errors and subjected to change.

This part is devoted to the proof of a famous theorem of Hasse's about the number of points on elliptic curve that are rational over a finite field. So the setting is that E is an elliptic curve defined over the finite field $\mathbb{F}_q$ where $q = p^r$ is a prime power—for simplicity, you may well assume that $q = p$. The question is:

Can you say something reasonable of the number $\#E(\mathbb{F}_q)$?

And, indeed one can, and there is a very suggestive heuristics about it. Let $y^2 = g(x)$ be the Weierstrass equation of the curve (so the coefficients are in $\mathbb{F}_q$). Half of the elements in $\mathbb{F}_q$ are squares, but each one has two square roots (except 0) so there are exactly q point of the form (y^2, x). Assuming that the polynomial $g(x)$ behaves well, that is the distribution among the x-values such that $g(x)$ has a square root or not is about $50 - 50$, one should suspect that there are about $q + 1$ points in $\#E(\mathbb{F}_Q)$ (the 1 comes from the point at infinity). Hasse's theorem states that is in fact a good guess, the discrepancy between $\#E(\mathbb{F}_q)$ and $q+1$ is no more than $2\sqrt{q}$. If q is big, the approximation is good. For example if q is of the order 10^6, which finally is not very big, the relative error is of the order one in thousand.

Theorem 5.1 *Let $q = p^r$ be a prime power and let E be an elliptic curve over the field $\mathbb{F}_q$. Then*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

EXAMPLE 5.1. This example is about the elliptic curve $y^2 = x^3 + x + 1$ over finite fields $\mathbb{F}_{101}$ with powers of $p = 101$. We have computed the number $N_q = \#E(\mathbb{F}_q)$ of rational points over $\mathbb{F}_q$ for the nine first successive powers 101^n of the prime 101 (and for $q = 101^{300}$ just to be convincing). Nowadays such computations are done in second using computer systems like *e.g.*, SAGE. One sees in column three that the fraction between the true error term $\alpha_q = q + 1 - N_q$ and the estimate $2\sqrt{q}$ stays relatively close to one, but that the relative error (column four) tends rapidly to zero.

n	N_q	$(q+1-N_q)/2\sqrt{q}$	$2\sqrt{q}/N_q$
1	90	0.597022	0.223 330 569 35
2	10260	-0.287128	0.019 688 109 16
3	1032210	-0.939866	0.001 966 726 61
4	104077440	-0.835114	0.000 196 027 11
5	10510112250	-0.057296	0.000 019 508 59
6	1061518570740	0.76669	0.000 000 194 11
7	107213515065810	0.766699	0.000 000 019 31
8	10828566974108160	0.972769	0.000 000 001 92
9	1093685273732923290	0.394831	0.000 000 000 19
	⋮		
	⋮		
300	197884662619.....	0.955896	0.000 000 000 00

❄

PROBLEM 5.1. Show that there is an exact sequence of multiplicative groups:

$$1 \longrightarrow \mu_2 \longrightarrow \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^* \longrightarrow \mu_2 \longrightarrow 1$$

Conclude that exactly half the members of $\mathbb{F}_q^*$ are squares. Show that -1 has a square root if and only if $q \equiv 1 \mod 4$. Conclude that -1 has a square root in $\mathbb{F}_{p^2}$ for all odd primes p. ✸

PROBLEM 5.2. Show that if $q \not\equiv 1 \mod n$, then every element of $\mathbb{F}_q$ has a unique n-th root. ✸

The proof of Hasse's theorem is rather easy once one has the full theory of isogenies, or at least significant part of it, at ones disposal, so the exposition starts with that. At the end comes the proof of Hasse's theorem, and it is so simple one might feel it as an anticlimax.

5.1 Isogenies

Let E and E' be two elliptic curves over the field k. They are both abelian groups having neutral elements O and O' respectively. Recall that an isogeny between them is a regular map $\phi\colon E \to E'$ that respects the neutral elements, *i.e.*, $\phi(O) = O'$. It is a fact, slightly astonishing however, that such a regular map ϕ automatically is a group homomorphism.

Over the complex numbers this is rooted in the curves having $\mathbb{C}$ as their universal covering spaces. They are represented as quotient $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ with lattices Λ and Λ' both as Riemann surfaces and abelian groups, and the map ϕ lifts to analytic map $\mathbb{C}$ that one shows is the multiplication by a complex number and hence additive. But as already announced, the result holds generally true:

Proposition 5.1 *Assume that E and E' are elliptic curves over the field k and that $\phi\colon E \to E'$ is an isogeny defined over k. Then ϕ is a group homomorphism; that is, $\phi(P+Q) = \phi(P) + \phi(Q)$ for all points $P, Q \in E$.*

PROOF: We use the identification of the group $E(k)$ with the group $\operatorname{Div}^0 E$ of divisors of degree 0 on E. This goes via the assignment $P \mapsto D = P - O$. Now, the map ϕ induces a map $\phi_*\colon \operatorname{Div}^0 E \to \operatorname{Div}^0 E'$ by sending a divisor $D = \sum_P n_P P$ to $\phi_* D = \sum n_P \phi(P)$. This is a group homomorphism, and as $\phi(O) = O'$, one has $\phi(P - O) = \phi(P) - O'$. The following diagram, where the horizontal maps are group isomorphisms, therefore commutes, and we are done:

$$\begin{array}{ccc} E(k) & \xrightarrow{\simeq} & \operatorname{Div}^0 E \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi_*} \\ E'(k) & \xrightarrow[\simeq]{} & \operatorname{Div}^0 E' \end{array}$$

❑

The set isogenies from E to E' will be denoted by $\operatorname{Hom}(E, E')$. As for any abelian groups, it is an abelian group under the usual addition defined by $(\phi + \psi)(x) = \phi(x) + \psi(x)$. In case $E' = E$, one writes $\operatorname{End}(E)$ for $\operatorname{Hom}(E, E)$, and its elements are called *endomorphisms of E*. Composition gives $\operatorname{End}(E)$ a ring structure.

PROBLEM 5.3. Assume that E is an elliptic curve over $\mathbb{C}$. Show that $\operatorname{End}(E)$ is a subring of $\mathbb{C}$ containing $\mathbb{Z}$, and hence commutative. From this originate the notion that E has *complex multiplication* if $\operatorname{End}(E) \neq \mathbb{Z}$. ✸

PROBLEM 5.4. Let E be the complex elliptic curve given by $\Lambda = \mathbb{Z} \oplus \mathbb{Z}i = \mathbb{Z}[i]$. Show that E has complex multiplication. Show that $\operatorname{End}(E) = \mathbb{Z}[i]$. ✸

PROBLEM 5.5. Let $\rho = \exp 2\pi i/3$. Show that the elliptic curve given by the lattice $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\rho$ has complex multiplication. What is $\operatorname{End}(E)$? ✸

PROBLEM 5.6. Assume k to be a field of characteristic different from 2. Assume that there is an element $i \in k$ such that $i^2 = -1$. Let E the curve given by $y^2 = x^3 + ax$ where $a \in k$ is non-zero. Show that E has an endomorphism ι such that $\iota^2 = -\mathrm{id}_E$ (the $-$ is the $-$ in the elliptic curve, so $-\mathrm{id}_E(x, y) = (x, -y)$). HINT: Use the map $(x, y) \to (-x, iy)$. ✸

PROBLEM 5.7. Assume k to be a field of characteristic different from 2 and 3. Assume that there is an element $\rho \in k$ such that $\rho^3 = 1$. Let E the curve given by $y^2 = x^3 + a$ where $a \in k$ is non-zero. Show that E has an endomorphism r such that $r^3 = \mathrm{id}_E$. HINT: Use the map $(x, y) \to (\rho x, y)$. ✸

THE DEGREE OS A REGULAR MAP It is a deep and fundamental theorem in algebraic geometry that any non-constant map $\phi\colon C \to C'$ between to complete curves C and C' is finite—in fact, it holds for maps between two complete varieties of the same dimension. This means that for any open $U \subseteq C'$ with ring of regular functions A, the ring of regular functions B on $\phi^{-1}U$ is a finite extension of A.

In particular the extension $K(C') \subseteq K(C)$ is finite, and its degree is called the *degree of ϕ* and is denoted by $\deg \phi$. For a constant map one declares the degree to be zero.

Suppose we are given another non-constant map ψ composable with ϕ, say $\psi\colon C' \to C''$. The three function fields constitute a tower of fields

$$K(C'') \subseteq K(C') \subseteq K(C),$$

and as the degrees of field extensions behave multiplicatively in tower, one has, after remarking that any composition with a constant map is constant, the following lemma:

DegMultiplikativ

Lemma 5.1 *Assume that ϕ and ψ are composable maps between complete curves. Then*

$$\deg \phi \circ \psi = \deg \phi \deg \psi.$$

The field extension $K(C') \subseteq K(C)$ may be split into the tower $K(C') \subseteq K \subseteq K(C)$ where $K(C') \subseteq K$ is the separable closure of $K(C')$ in $K(C)$. One shows that the composite of two separable field extensions is separable, so there is a largest separable extension, and this is the separable closure. Hence $K \subseteq K(C)$ is *purely inseparable*, no element in $K(C)$ is separable over K.

Any regular map ϕ may be written as a composition $\phi = \phi_s\phi_i$ with ϕ_s separable and ϕ_i purely inseparable, and the degree can correspondingly be factored as $\deg \phi = \deg \phi_s \deg \phi_i$.

The degree has another more geometric interpretation, at least in the case ϕ is separable. Then general theory tells us that the degree is equal to the number of elements in a generic fibre. Ramification points can of course occur, but they are finite in number and away from those, the fibres contain exactly $\deg \phi$ points. To be precise, there is a non-empty open subset $U \subseteq C'$ such that all the fibres $\phi^{-1}(x)$ with $x \in U$ has exactly $\deg \phi$ points.

In the case of elliptic curves a translation trick allows us to say more. We have

Lemma 5.2 *Assume that $\phi\colon E' \to E$ is a separable isogeny between the two elliptic curves E and E'. For any point $P \in E$, the number of points in the fibre $\phi^{-1}(P)$ is equal to the degree $\deg\phi$. In particular the degree is equal to the order of $\operatorname{Ker}\phi$.*

PROOF: This follows from the commutative diagram

$$\begin{array}{ccc} E' & \xrightarrow{\tau_{P'}} & E' \\ \downarrow{\scriptstyle\phi} & & \downarrow{\scriptstyle\phi} \\ E & \xrightarrow{\tau_P} & E \end{array}$$

where $P' \in E'$ is a point with $\phi(P') = P$, and τ_P are the translation maps. The diagram commutes since ϕ being a group homomorphism, one has $\phi(P' + x) = \phi(P') + \phi(x) = P + \phi(x)$. The translation map τ_P sends O to P and $\tau_{P'}$ therefore induces a bijection between $\operatorname{Ker}\phi = \phi^{-1}(O)$ and the fibre $\phi^{-1}(P)$. For a generic point P in E, general theory tells us that the fibre has exactly $\deg\phi$ points. ❑

EXAMPLE 5.2. — MULTIPLICATION BY m. Let $m \in \mathbb{Z}$ be an integer. As E is a group, we have the multiplication-by-m map $[m]\colon E \to E$ with $[m]P = P$, which plays a particular important role. Clearly $[m]$ is an isogeny, an the assignment $m \to [m]$ is a ring homomorphism $\mathbb{Z} \to \operatorname{End}(E)$. Indeed, is obvious that one has $nmP = n(mP)$ and $(n+m)P = nP + mP$ so it behaves well with respect to the algebraic operations. It is slightly more subtle that the map is injective, *i.e.,* that $[m]$ is never constant:

Lemma 5.3 *For any $m \in \mathbb{Z}$, the multiplication-by-m map $[m]$ is not the zero map.*

PROOF: From general principles it follows that the derivative of $[m]$ at O is multiplication by m in the tangent space $T_O E$. Hence the derivative of $[m]$ is not zero and $[m]$ is not constant at least as long as the characteristic p of k does not divide m.

In the process of bringing every elliptic curve on Weierstrass form, we checked that over an algebraically closed field there is exactly four two-torsion points if the characteristic is not 2, and in that case there are at most one. Anyhow, as $E(k)$ has infinitely many points, not all can be two-torsion, and the multiplication-by-two map $[2]$ is not constant. The composition of surjective maps is surjective and therefore $[2^r] = [2]^r$ is not constant whatever the natural number r is, so we are done if the characteristic is 2 by factoring $m = 2^r n$ with n odd.

Assume that $[p] = O$ and that $p \neq 2$. Then $[-1] = [p-1] = [2r]$ for some r that obviously does not have p as a factor, and we get the contradiction $1 = \deg[-1] = \deg[2]\deg[r] = 4\deg[r] > 1$. Hence $[p]$ is not constant neither is $[p^r]$, and therefore by factoring m as $m = p^r n$ with $(p, n) = 1$ we are through. ❑

❄

EXAMPLE 5.3. — THE FROBENIUS ENDOMORPHISM. The Frobenius map is ubiquitous in number theory, it is indispensable when you want to count points on a variety rational over a finite field. It plays the leading role in the xxxx.

Let p be a prime and let k be a field of characteristic p. For example k can be one of the finite fields $\mathbb{F}_q$ with $q = p^r$ elements or their algebraic closure $\mathbb{F}$. The function field $K(E)$ of an elliptic curve defined over $\mathbb{F}$ is another example we shall meet.

Recall that the map $\theta\colon k \to k$ rising an element to the p-th power— that is $\theta(a) = a^p$—is a ring homomorphism. To precise, the field k should be visible in the notation and one should write θ_k, but we systematically break that rule since the field is almost always clear from the context.

It is no miracle that θ is multiplicative, but its additivity is more subtle and is due to the vanishing of the binomial coefficients $\binom{n}{p}$. The map θ is named after the great german mathematician Ferdinand Georg Frobenius who lived from 1849 to 1917. In Galois theory there is also a number of automorphisms of number fields bearing his name. They are all lifts of the maps in characteristic p we described above.

Fermat's little theorem tells us that if $a \in \mathbb{F}_p$, then $\theta(a) = a$. The converse is true as well since the equation $x^p - x$ has at most p solutions. Similarly, the fixed field of the iterated Frobenius map θ^r, is the field $\mathbb{F}_q$ with $q = p^r$, elements. Indeed, the equation $x^q - x$ is separable (the derivative is -1) and has therefore exactly q roots.

PROBLEM 5.8. Show that any two fields with $q = p^r$ elements are isomorphic extensions of $\mathbb{F}_p$. HINT: They are both root fields of $x^q - x$. ✸

After this small excursion to the finite fields, we rush back to our main objects of study. Let E an elliptic curve over an algebraically closed field k of characteristic p, the basic example being $\mathbb{F}$. Assume that E is given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a^4x + a^6 = g(x).$$

where we have used the extended version to include the cases $p = 2$ and $p = 3$. Replacing every coefficient in the Weierstrass equation by its q-th power, we obtain a new elliptic curve $E^{(p)}$ with equation

$$y^2 + a_1^p xy + a_3^p y = x^3 + a_2^p x^2 + a_4^p x + a_6^p.$$

The discriminant of $E^{(p)}$ is the p-th power of the one of E, so $E^{(p)}$ is smooth. The Frobenius map induces an isogeny $\theta_E\colon E \to E^{(p)}$ that sends a point (x, y) of E to (x^p, y^p), and the point at infinity of course goes to the point at infinity. This isogeny is called the *Frobenius isogeny*.

FrobSep

Lemma 5.4 *The Frobenius map $\theta_E\colon E \to E^{(p)}$ is purely inseparable and of degree p.*

PROOF: Let x and y be Weierstrass coordinates on E. First assume that $p \neq 2$. Then x and y satisfy a Weierstrass equation $y^2 = g(x)$, and the extension of function fields corresponding to the Frobenius map θ_E is $k(x^p, y^p) \subseteq k(x, y)$. Now p is odd so we may

write $p = 2r + 1$. Hence $y = y^p y^{-2r} = y^p g(x)^{-2r}$. This shows that $k(x, y) = k(x, y^p)$, and that the extension $k(x^p, y^p) \subseteq k(x, y)$ is generated by x, whose minimal equation is $T^p - x^p$.

In case $p = 2$, either a_1 or a_3 is non-zero since E is smooth. So one has $y = (g(x) - y^2)(a_1 x + a_3)^{-1}$ and $k(x, y) = k(x, y^2)$. Again, $k(x, y)$ is generated by x over $k(x^2, y^2)$, and the minimal equation is $T^2 - x^2$. ❑

One may iterate the Frobenius construction and for every power $q = p^r$ arrive at a curve $E^{(q)}$ and regular map $\theta_E^r \colon E \to E^{(q)}$. From lemma 5.4 above, by an immediate induction, follows that θ_E^r is purely inseparable of degree q.

There is a converse to lemma 5.4:

FactorSepFrob

Lemma 5.5 *Assume that $\phi : E \to E'$ is purely inseparable isogeny of degree $q = p^r$. Then up to an isomorphism of E' one has $\phi = \theta_E^r$. Hence any isogeny $\phi \colon E \to E'$ factors as $\phi = \phi_s \theta_E^r$ where ϕ_s is separable.*

PROOF: The first remark is that $k(x^q, y^q) = \{\, a^q \mid a \in k(x, y) \,\}$ since the base field k is perfect (any of its elements is a q-power). Since $k(x, y)$ is purely inseparable of degree q over $K(E')$, both x^q and y^q lie in $k(E')$ (they satisfy equations of type $T^{p^{r'}} - a$ with $a \in K(E')$ and $r' \leq r$) and $k(x^q, y^q) \subseteq K(E')$. But we just saw that $k(x, y)$ is of degree q over $k(x^q, y^q)$, hence $k(x^q, y^q) = K(E')$. ❑

If the elliptic curve E is defined over the prime field $\mathbb{F}_p$, we may find a Weierstrass equation all whose coefficients belong to $\mathbb{F}_p$. The curves E and $E^{(p)}$ then coincide since $a_i^p = a_i$, and the Frobenius becomes an *endomorphism* of E. The same goes with the powers θ^r whenever E is defined over the field $\mathbb{F}_q$ with $q = p^r$ elements; indeed, in that case $\theta^r(a_i) = a_i^q = a_i$.

The following result is fundamental when it comes to counting the number of points in $E(\mathbb{F}_q)$:

Lemma 5.6 *Assume that the elliptic curve E is defined over $\mathbb{F}_q$ where $q = p^r$. The isogeny $1 - \theta_E^r$ is separable, and one has*

$$E(\mathbb{F}_q) = \operatorname{Ker}(1 - \theta_E^r).$$

Hence $\#E(\mathbb{F}_q) = \deg(1 - \theta_E^r)$.

PROOF: The derivative of $1 - \theta_E^r$ is the identity, since $D_O \theta_E = 0$, and $1 - \theta^r$ is separable. The coordinates $P = (x, y)$ of a point in $E(\mathbb{F})$ lie in $E(\mathbb{F}_q)$ if and only if $x^q = x$ and $y^q = y$, that is if and only if $\theta_E(x, y) = (x, y)$, *i.e.*, $(\theta_E - 1)P = O$. ❑

The Frobenius construction is functorial in the sense that if $\phi \colon E \to F$ is an isogeny, there is a unique isogeny $\phi^{(q)} \colon E^{(q)} \to F^{(q)}$ making the following diagram commutative:

$$\begin{array}{ccc} E & \xrightarrow{\phi} & F \\ {\scriptstyle \theta_E^r}\downarrow & & \downarrow{\scriptstyle \theta_F^r} \\ E^{(q)} & \xrightarrow[\phi^{(q)}]{} & F^{(q)} \end{array} \qquad (\bigstar)$$

FrobIsog

Indeed, one may express the Weierstrass coordinates x' and y' of F in terms of those on E as $x' = \Phi_1(x, y)$ and $y' = \Phi_2(x, y)$ where each Φ_i is a rational function with coefficients in k. Let $\Phi_i^{(q)}$ denote the rational function obtained by rising all the coefficients of Φ_i to the q-th power, and let $\phi^{(q)}$ be the map whose components are the $\Phi_i^{(q)}$.

We claim that ϕ^q takes points of $E^{(q)}$ into points of $F^{(q)}$. Indeed, if $(x, y) \in E^q$ one may write $x = x_1^q$ and $y = y_1^q$ with $x_1, y_1 \in k$. (k algebraically closed). Then the Weierstrass relation $\Phi_2(x_1, y_1)^2 = g(\Phi_1(x_1, y_1))$ implies that $\Phi_1^{(q)}(x, y)^2 = g^{(q)}(\Phi_2^{(q)}(x, y))$ where $g^{(q)}$ is the polynomial g with all coefficients risen to the q-power.

From the diagram (✯) we arrive at

$$(1 - \theta_F^r)\phi = \phi^{(q)}(1 - \theta_E^r).$$

Taking degrees and cancelling $\deg \phi$ one sees that $\deg(1 - \theta_F^r) = \deg(1 - \theta_E^r)$. Hence

Proposition 5.2 *Assume that E and F are isogenous elliptic curves over $\mathbb{F}$. Then for every q they have the same number of rational points over $\mathbb{F}_q$; i.e., $\#E(\mathbb{F}_q) = \#F(\mathbb{F}_q)$*

❄

5.1.1 The formation of quotients

Assume that $G \subseteq E$ is a finite group. Just as in the theory of groups, one wants to have the quotient E/G. It certainly exists as an abelian group, but we want as an elliptic curve and we want the quotient map to be regular. And all these wishes are fulfilled:

EksistesKvotient

Proposition 5.3 *Let E be an elliptic curve over k, and let $G \subseteq E(k)$ be a finite group. Then there is an elliptic curve E/G with origin $O' = \pi(O)$, and a separable isogeny*

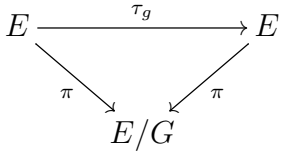
$$\pi\colon E \to E/G$$

with $\operatorname{Ker}\pi = G$. One has $\deg\pi = |G|$. This construction is unique in the sense that if $\phi\colon E \to E'$ is an isogeny with $\operatorname{Ker}\phi = G$, then there is an isomorphism $\alpha\colon E/G \simeq E'$ such that $\alpha\pi = \phi$.

PROOF: The subgroup G acts on E by the translations τ_g, given as $\tau_g(P) = P + g$. These maps are regular and the action of G on E therefore induces an action of G on the function field $K(E)$. Let $K = K(E)^G$ be the fixed field. Galois theory tells us that $K(E)$ is an extension of K that is separable and finite of degree $|G|$.

By general theory there is a smooth and projective curve—that we denote by E/G—and a separable, regular map $\pi\colon E \to E/G$ of degree $|G|$ such that π^* identifies $K(E/G)$

with the subfield K of $K(E)$. As G acts trivially on K, one has $\pi\tau_g = \pi$, that is, one has commutative diagrams



The most salient point of the proof, is to show that E/G is of genus one. This will follow once we show that the map π is unramified. Indeed, if $P \in E/G$, then the fibre $\pi^{-1}(P)$ contains the set $A = \{ P+g \mid g \in G \}$ since $\pi\tau_g = \pi$. Now surely $P+g = P+g'$ implies that $g = g'$, so the set A has exactly $|G|$ elements in it, one for each $g \in G$. It follows that the fibre equals A, and we can conclude that *all* fibres consist of $\deg\pi$ different elements—which is equivalent to π being unramified.

Letting $\pi(O)$ be the origin in E/G, it becomes an elliptic curve and π an isogeny. Finally, one easily checks that $\operatorname{Ker}\phi = G$ using $\pi\tau_g = \pi$ once more.

Since $\operatorname{Ker}\phi = G$, the map ϕ identifies $K(E')$ as a subfield of $K(E)^G$, and the $[K(E) : \phi^*K(E')] = \deg\phi = |\mathrm{Ker}|\phi = |G| = [K(E) : K(E)^G]$, it follows that $K(E') = K(E)^G = K(E/G)$ and the statement about uniqueness follows. ❑

5.1.2 The dual isogeny

The principal tool in the proof of the Hasse theorem is a quadratic form on the group $\mathrm{End}(E)$. This form is best defined in terms of what is called *dual isogenies*. To every isogeny $E \to E'$ we are going to construct another one $\hat{\phi}$ that goes the other way—*i.e.*, $\hat{\phi}\colon E' \to E$—called the *dual isogeny*. The defining property of $\hat{\phi}$ will be $\hat{\phi}\circ\phi = [\deg\phi]$.

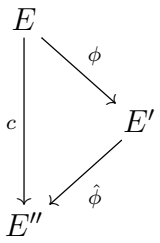
In other part of mathematics one often has a quadratic form or scalar product of some sort, and then defines "dual maps" , like for example transposed matrices or adjoint linear maps. But here it is convenient to do it the other way around: First construct the dual objects and subsequently extract the scalar product from them !

Proposition 5.4 *Given an isogeny $\phi\colon E \to E'$ of degree $\deg\phi$. Then there exists a unique isogeny $\hat{\phi} : E' \to E$ with $\hat{\phi}\circ\phi = [\deg\phi]$*

PROOF: One easily checks that if ϕ has the dual $\hat{\phi}$ and ψ has the dual $\hat{\psi}$, then $\hat{\psi}\hat{\phi}$ is the dual of $\phi\psi$. Hence once we have constructed the dual of any separable isogeny and of the Frobenius θ, we are done, by lemma 5.5.

Assume first that ϕ is separable, and to ease notation, put $m = \deg\phi$. The kernel $\operatorname{Ker}\phi$ has m elements and is consequently annihilated by m. Hence $\operatorname{Ker}\phi \subseteq E_m = \operatorname{Ker}[m]$. Let $G \subseteq E'$ be the subgroup $E_m/\operatorname{Ker}\phi = \phi(E_m)$. This is clearly a finite group, and we may form the quotient $E'' = E'/G$, denoting the quotient map by $\hat{\phi}$. There is

the commutative the diagram, where $c = \hat{\phi}\phi$:



Now, the kernel of the composition c is $E_m = \mathrm{Ker}[m]$, and after the uniqueness statement in proposition 5.3 on page 8 one has $E'' = E$ and $c = [m]$ up to isomorphism (if necessary, change $\hat{\phi}$ by an automorphism).

In the case of the Frobenius θ , which is of degree p, we start with factoring the multiplication-by-p map $[p]$ as a composition of a separable isogeny α and a power of the Frobenius; *i.e.,* $[p] = \alpha\theta^r$. This can be done according to lemma 5.5, and the exponent r is greater than one since $[p]$ is inseparable. Then $\hat{\alpha}\theta^{r-1}$ will do as the dual $\hat{\theta}$, since we obviously have $\hat{\alpha}\theta^{r-1}\theta = [p]$.

The isogeny $\hat{\phi}$ is unique: If $\psi\phi = \hat{\phi}\phi = [m]$, then $(\psi - \hat{\phi})\phi = 0$, but ϕ being surjective, this implies that $\psi - \hat{\phi} = 0$. ❑

The isogeny $\hat{\phi}$ is called the *dual isogeny of* ϕ. In the case $E' = E$, the dual $\hat{\phi}$ maps E to E as well, and $\hat{\phi} \in \mathrm{End}(E)$. The "hat" therefore is an involution on the ring $\mathrm{End}(E)$. It is called the *Rosati involution* after the italian mathematician Carlo Rosati. The formal definition of an involution is that it should be a ring homomorphism whose square is the identity, and in the next proposition we verify this among several other properties of the dual isogeny.

DuaslProperts

Proposition 5.5 *Let ϕ and ψ be isogenies that either can be composed or added (according to the different requirement of the statements). One has*

- $\widehat{(\psi + \phi)} = \hat{\psi} + \hat{\phi}$
- $\hat{\phi}\phi = \phi\hat{\phi} = [\deg \phi]$
- $\widehat{(\phi\psi)} = \hat{\psi}\hat{\phi}$
- $\widehat{[m]} = [m]$ *and* $\deg[m] = m^2$
- $\deg \hat{\phi} = \deg \phi$ *and* $\hat{\hat{\phi}} = \phi$

PROOF: The only substantial statement is the first statement about the additivity of the "hat", the rest follows formally from this. Normally the additivity is proved in the more general context of abelian varieties, and the proof relies on two results respectively called the theorem of the square and the theorem of the cube. There are proofs in our

context, but to our taste they are gnarled and not very enlightening, so we refrain from giving one and shall only do the (easy) formalities

So we start with the second statement. The isogeny ϕ being a group homomorphism, it commutes with any multiplication map $[m]$; hence one has

$$\phi\hat{\phi}\phi = \phi[\deg\phi] = [\deg\phi]\phi.$$

Since ϕ is surjective, it can be cancelled from the right, and we arrive at $\phi\hat{\phi} = [\deg\phi]$.

The second now follows as

$$\hat{\phi}\hat{\psi}\psi\phi = \hat{\phi}[\deg\psi]\phi = [\deg\psi]\hat{\phi}\phi = [\deg\psi][\deg\phi] = [\deg\psi\phi]$$

The forth is an easy induction on m. By the additivity and induction we have

$$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]} = [m] + [1] = [m+1].$$

The statement about $\deg[m]$ follows by induction as well, via the following elementary calculation:

$$\begin{aligned}\widehat{[m+1]}[m+1] = [m+1][m+1] = ([m]+[1])([m]+[1]) = [m][m] + 2[m] + [1] \\ = [\deg[m] + 2m + 1] = [m^2 + 2m + 1] = [(m+1)^2].\end{aligned}$$

That $\deg\hat{\phi} = \deg\phi$ is now clear, indeed

$$\deg\hat{\phi}\phi = \deg\hat{\phi}\deg\phi = \deg[\deg\phi] = (\deg\phi)^2$$

❑

Proposition 5.6 *Let k be algebraically closed. Assume that m is prime to characteristic of k and that E is an elliptic curve over k. Then $E_m(k) \simeq (\mathbb{Z}/m\mathbb{Z})^2$.*

PROOF: We know that for any divisor n of m the multiplication-by-n map $[n]$ is separable and of degree n^2. Hence $|\mathrm{Ker}[n]| = |E_n(k)| = n^2$. Indeed, this follows since if l is a prime factor in m, the l-primary part of $E_m(k)$ is a direct sum $\bigoplus \mathbb{Z}/l^i\mathbb{Z}$ with say s summands, so on one hand $E_l(k)$ is of order l^s but on the other $E_l(k)$ of order l^2, so $s = 2$. ❑

The quadratic form on $\mathrm{End}(E)$

In general, let A be an abelian group and let $q\colon A \to \mathbb{Z}$ be a function. We say say q is a *quadratic function*

- ☐ $q(-a) = q(a)$ for all $a \in A$
- ☐ The form $\langle a, b \rangle = q(a+b) - q(a) - q(b)$ is bilinear.

The last request mimics the so called "polarization formula" for a scalar product, in its simplest form it is just the identity $2xy = (x+y)^2 - x^2 - y^2$. In the setting above, A is just a group and there is no reason for elements to be divisible by 2, hence the factor 2 is kept in the polarization formula. One could be tempted to extend the scalars and replace A by $A \otimes \mathbb{Q}$ to be in standard situation with quadratic form on a vector space over a field.

Clearly the expression for $\langle a, b \rangle$ is symmetric in a and b, so once it is bilinear, $\langle a, b \rangle$ will be a "scalar product" on A.

One easily verifies that $q(0) = 0$—by bilinearity $\langle 0, 0 \rangle = 0$, and hence $q(0) = 2q(0)$— and one has $\langle a, a \rangle = 2q(a)$. Indeed, adding the two identities

$$\begin{aligned} -\langle x, x \rangle = \langle -x, x \rangle &= q(0) - 2q(x) \\ \langle x, x \rangle &= q(2x) - 2q(x) \end{aligned}$$

one obtains $q(2a) = 4q(a)$, and hence $\langle a, a \rangle = 2q(a)$.

Proposition 5.7 *Let E an elliptic curve over k. $\langle \phi, \psi \rangle = q(\phi + \psi) - q(\phi) - q(\psi)$ is a positive definite quadratic form on $\mathrm{End}(E)$ with $\langle \phi, \phi \rangle = 2 \deg \phi$*

PROOF: This is where the dual isogeny comes into play: We compute

$$\begin{aligned} [\deg(\phi + \psi) - \deg \phi - \deg \psi] &= \widehat{(\phi + \psi)}(\phi + \psi) - \hat{\phi}\phi - \hat{\psi}\psi = \\ &= (\hat{\phi} + \hat{\psi})(\phi + \psi) - \hat{\phi}\phi - \hat{\psi}\psi = \hat{\phi}\psi + \hat{\psi}\phi. \end{aligned}$$

The last expression is clearly linear in both ϕ and ψ thanks to the first property in 5.5 on page 10 and since $[n] = [m]$ implies $n = m$, we are done. The equality $\langle \phi, \phi \rangle = 2 \deg \phi$ is just the generalities we explained above. By definition $\deg \phi \geq 0$, and the only isogeny of degree 0 is $[0]$! ❑

A fundamental result on inner products is the Cauchy-Schwarz inequality which states that

$$|\langle a, b \rangle| \leq \sqrt{\|a\| \, \|b\|}$$

where the norm an element is $\|a\| = \langle a, a \rangle$. In our slightly more general situation it is of course still valid, but there is factor 2 appearing due to the factor 2 in the polarization formula:

Proposition 5.8 (Cauchy-Schwarz) *Then*

$$\langle \phi, \psi \rangle \leq 2 \deg \phi \deg \psi$$

Proof of Hasse's theorem

Theorem 5.2 *Let E be an elliptic curve over the field $\mathbb{F}_p$. Then*

$$|q + 1 - N_q| \leq 2\sqrt{q}$$

PROOF: Once the theory of the isogenies is established this is a direct application of the inner product on $\mathrm{End}(E)$ and the Cauchy-Schwarz inequality. One computes

$$\begin{aligned} 2\#E(\mathbb{F}_q) &= 2\deg([1]-\theta) = \\ &= \langle\, [1]-\theta, [1]-\theta \,\rangle = \\ &= \langle\, [1],[1] \,\rangle - 2\langle\, [1],\theta \,\rangle + \langle\, \theta,\theta \,\rangle = \\ &= 2\deg[1] - 2\langle\, [1],\theta \,\rangle + 2\deg\theta = \\ &= 2 - 2\langle\, [1],\theta \,\rangle + 2q \end{aligned}$$

Hence

$$|q+1-\#E(\mathbb{F}_q)| = |\langle\, [1],\theta \,\rangle| \leq 2\sqrt{\deg[1]\deg\theta} = 2\sqrt{q}$$

❑

PROBLEM 5.9. Let E have equation $y^2 = x^3 + a$ with $a \in k$ non-zero. Show that if $q \not\equiv 1 \mod 3$, then $\#E(\mathbb{F}_q) = q+1$. HINT: Every element in $\mathbb{F}_q$ has a unique cube root. ✸

Appendix

5.1.3 The derivative of the addition map

Any variety X has a tangent spaces $T_{X,x}$ at smooth points x. At a point $x \in X$ (assumed to be smooth) it equals the k-vector space $(\mathfrak{m}/\mathfrak{m}^2)^*$ dual to the space $\mathfrak{m}_x/\mathfrak{m}_x^2$.

The intuition being as follows. Take a function f defined near x and assume that $f(x) = a$. One may write $f = a + df \mod \mathfrak{m}^2$ where $df \in \mathfrak{m}_x/\mathfrak{m}_x^2$. This is just what is left of a Taylor-development when one disregards terms of degree 2 or more. In analogy with what we learned in calculus courses, df is corresponds to the gradient ∇f. The directional derivative along a vector v is just $v\cdot\nabla f$, *i.e.,* the value of the linear functional $w \mapsto v\cdot w$ on the gradient. So linear functionals on the space of possible quadratic terms in Taylor-developments correspond to "directions", that is tangent vectors.

If $\phi\colon X \to Y$ is a regular map with $\phi(x) = y$, both points being smooth, there is induced a derivative $D_x\phi = T_{X,x} \to T_{Y,\phi(x)}$ which is a k-linear map. This simply because the ring homomorphism $f \to f\circ\phi$ takes $\mathfrak{m}_x$ into $\mathfrak{m}_{\phi(x)}$. The derivative satisfies the chain rule: $D_{f(x)}f \circ g_x D = D_{f(g(x))}f \circ g$.

For varieties over $\mathbb{C}$, this definition coincides of course both with the one from differential geometry and the analytic one.

The tangent space of $E\times E$ at $(0,0)$ is in a natural way identified with $T_{E,0}\oplus T_{E,0}$. If ι_1 and π_1 respectively denotes the projection onto the first factor and the inclusion $\iota_1(P) = (P,0)$, the first summand in the splitting of $T_{(0,0)}E\times E$ lies split via $D_0\iota_1$ and $D_{(0,0)}\pi_1$; indeed, $\pi_1\circ\iota_1 = \mathrm{id}$, so the chain rule gives $D_{(0,0)}\pi_1 \circ D_0\iota_1 = \mathrm{id}$.

Let t be a parameter at the origin $0 \in E$, that is t generates $\mathfrak{m}_0/\mathfrak{m}_0^2$. The dual of t in T_0E is denoted by dt. The two elements $t_i = D_0\iota_i(dt)$ form a basis for the tangent space $T_{(0,0)}E \times E$.

Now let $\mu\colon E \times E \to E$ be the addition map. One has

Lemma 5.7 *The derivative of $D_{(0,0)}\mu$ of μ at $(0,0)$ is the addition map $T_0E \oplus T_0E \to T_0E$.*

PROOF: One may write $D_{(0,0)}t_j = \alpha_j dt$. As $\mu \circ \iota_j = \mathrm{id}_E$, one finds $dt = D_0\mu \circ \iota_j(dt) = D_{(0,0)}\mu(t_j)$. ❑

Lemma 5.8 *The derivative $D_0[m]$ of the multiplication map $[m]$ is the multiplication map m, i.e., $D_0[m](v) = mv$ for all tangent vectors $v \in T_0E$.*

Lemma 5.9 *If p is the characteristic of k. Then $[m]$ is a separable map if and only if p does not divide m.*

PROOF: If $p \not| m$ the derivative of $[m]$ is an isomorphism at 0. By a translation argument shows it follows that it is iso everywhere. Indeed if $P \in E$, one has the commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\tau_P} & E \\ {\scriptstyle [m]}\downarrow & & \downarrow{\scriptstyle [m]} \\ E & \xrightarrow[\tau_{mP}]{} & E \end{array}$$

where the translations τ_P and τ_{mP} are isomorphisms. (the translation is given as $\tau_P(Q) = P + Q$). On the other hand, if $p|m$, the derivative vanishes at 0, and by the same translation argument above, it vanishes everywhere, that is to say, it is inseparable. ❑

5.1.4 Alternative approach

There are several ways of establishing this fact, and a completely different line of attack, is to appeal to a result of Mumford's called the ridgity lemma. It has the virtue of being very general and also work for so called abelian varieties, but it uses some algerian geometry, and in that sense is on the edge of this course. The ridgity lemma says basically that if a family of regular maps from a complete variety depending regularly on a parameter, is constant for one value of the parameter, then it is constant for all parameter values.

Lemma 5.10 *Assume that X, Y and Z are varieties over k with X being complete. Let $f\colon X \times Y \to Z$ be a regular map. and assume that $f(x, y_0)$ is constant. Then there is a map $g\colon Y \to Z$ such that $f(x, y) = g(y)$.*

PROOF: Let $f(x, y_0) = z_0$ and let $U \subseteq W$ be an affine open neigbourhood of z_0. Let T be the complement of $f^{-1}(U)$. Then T is closed and since X is complete, $\pi(T)$ is closed where $\pi\colon X \times Y \to Y$ denotes the second projection, and as $y_0 \notin T$, $V = Y \setminus T$ is non empty. Clearly f restricts to a map $X \times V \to U$, but X is complete and U is affine, so for each fixed y the map $f(x, y)$ is constant. ❑

To apply this lemma in our situation, we let $X = Y = Z = E$, and the map f will be $f(P+Q) = \phi(P+Q) - \phi(P) - \phi(Q)$. Since ϕ and the addition maps all are regular, this is a regular map. Of course $f(x, O) = \phi(P + O) - \phi(P) - \phi(O) = O'$ since $\phi(O) = O'$, so the hypothesises of the lemma are satisfied and conclude that $f(P, Q) = g(Q)$. Substituting $P = O$, we arrive at $g(Q) = f(P, O) = O'$ and we are done.